Dell SupportAssist Version 1.3 For Dell OpenManage Essentials
Quick Start Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 02

Rev. A00

Contents

1 Getting Started With SupportAssist....5
Setting Up OpenManage Essentials For SupportAssist....5
Configuring SNMP Services On Windows....6
Configuring SNMP Services on Linux....6
Installing SNMP Tools (Windows Server 2012 Or Later)....7
Enabling Network Discovery (Windows Server 2008 Only)....7
Setting Up SupportAssist....7
Ensuring Successful Communication Between The SupportAssist Application And The SupportAssist Server....8
Testing SupportAssist Connectivity....9
Verifying The Installation Of The Collection Tools....9
Configuring The Default Device Type Credentials....10
Configuring Periodic Collection Of System Logs....11
Verifying The System Log Collection Or Upload Configuration....12
Enabling Auto Update....12
Troubleshooting....12
Registration Failure....13
Collection Failure....13
Collection Upload Failure....13
Connectivity Test Failure....14

Getting Started With SupportAssist

Dell SupportAssist plugin for Dell OpenManage Essentials provides proactive support capabilities for supported Dell server, storage, and networking solutions. OpenManage Essentials interacts with supported devices that are to be monitored and receives SNMP traps. The SNMP traps are periodically retrieved as alerts by the SupportAssist application. The alerts are filtered using various policies to decide if the alerts qualify for creating a new support case or updating an existing support case.

All qualifying alerts are securely sent to the SupportAssist server hosted by Dell, for creating a new support case or updating an existing support case. After the support case is created or updated, the SupportAssist application, runs the appropriate collection tools on the devices that generated the alerts, and uploads the log collection to Dell. The information in the log collection is used by Dell technical support to troubleshoot the issue and provide an appropriate solution.

This document provides information required to ensure that SupportAssist works as expected in your environment. To quickly get started with SupportAssist, follow the instructions in Setting Up OpenManage Essentials For SupportAssist and Setting Up SupportAssist.

Setting Up OpenManage Essentials For SupportAssist

For SupportAssist to remotely monitor supported devices and automatically generate support cases if there is a hardware issue in your environment, you must set up OpenManage Essentials as follows:

1. Ensure that OpenManage Essentials version 1.3 is installed on the management server. For information on installing OpenManage Essentials, see the *Dell OpenManage Essentials Version 1.3 User's Guide* at **dell.com/OpenManageManuals**.
2. Configure SNMP services on all managed nodes. See Configuring SNMP Services On Windows and Configuring SNMP Services On Linux.

   NOTE: On managed nodes running Microsoft Windows Server 2012 or later, before configuring SNMP services, you must install SNMP tools. See Installing SNMP Tools.
3. On all managed nodes, ensure that Dell OpenManage Server Administrator (OMSA) is installed. For information on installing OMSA, see the *Dell OpenManage Server Administrator User's Guide* at **dell.com/OpenManageManuals**.

   NOTE: Dell PowerEdge 12G servers can provide statusing, alerts, and limited inventory through iDRAC even if OMSA is not installed.
4. On all managed nodes running Windows Server 2008, ensure that network discovery is enabled. See Enabling Network Discovery (Windows Server 2008 Only).
5. Configure the supported Dell devices in your environment so that they can be discovered and managed by OpenManage Essentials. For instructions to configure the supported Dell devices, see the *Making My Environment Manageable for Dell OpenManage Essentials* technical white paper at **DellTechCenter.com/OME**.
6. Verify the firewall configuration and ensure that the following ports are open:
   - On the management server, port 162 for SNMP; port 443 for SSL communication and for getting SupportAssist update information.
   - On the managed node, port 161 for SNMP and port 1311 for OMSA.
7. Discover and inventory the supported devices in your environment in OpenManage Essentials using the recommended protocols. For information on discovery and inventory of devices, see the *Dell OpenManage Essentials Version 1.3 User's Guide* at **dell.com/OpenManageManuals**.

Configuring SNMP Services On Windows

1. Open a command prompt, type `services.msc`, and press <Enter>.
   The **Services** window is displayed.
2. Browse the list of services, and ensure that the status of the **SNMP Service** is displayed as **Started**.
3. Right-click **SNMP Service** and select **Properties**.
   The **SNMP Service Properties** dialog box is displayed.
4. Click the **Security** tab and perform the following:

   NOTE: If the **Security** tab is not displayed, reopen the **Services** window and try again.

   a) Clear **Send authentication trap**.
   b) Under **Accepted community** names, click **Add**.
      The **SNMP Service Configuration** dialog box is displayed.
   c) From the **Community rights** list, select **READ ONLY**.
   d) In the **Community Name** field, type the community name and click **Add**.
   e) Select either **Accept SNMP packets from any hosts** or **Accept SNMP packets from these hosts**, and click **Add**.
      The **SNMP Service Configuration** dialog box is displayed.
   f) In the **Host name, IP or IPX address** field, type the OpenManage Essentials server name or IP address, and click **Add**.
5. Click the **Traps** tab, and perform the following:
   a) In the **Community name** box, type the community name, and click **Add to list**.
   b) Under **Trap destinations**, click **Add**.
      The **SNMP Service Configuration** dialog box is displayed.
   c) In the **Host name, IP or IPX address** field, type the OpenManage Essentials server name or address, and click **Add**.
6. Click **Apply**.
7. In the **Services** window, right-click **SNMP Service** and click **Restart**.

   NOTE: The default port for sending SNMP traps is 162. To configure the managed node to use a non-default port, see the "Changing the Default SNMP Port" section in the *Dell OpenManage Essentials Version 1.3 User's Guide* at **dell.com/OpenManageManuals**.

Configuring SNMP Services on Linux

1. Run the command `rpm -qa | grep snmp`, and ensure that the **net-snmp** package is installed.
2. Run `cd /etc/snmp` to navigate to the snmp directory.
3. Open **snmpd.conf** in the VI editor (**vi snmpd.conf**).
4. Search **snmpd.conf** for **# group context sec.model sec.level prefix read write notif** and ensure that the values for fields **read**, **write**, and **notif** are set to **all**.
5. At the end of the **snmpd.conf** file, just before **Further Information**, enter the OpenManage Essentials console IP address in the following format:`trapsink <OpenManage Essentials Console IP> <community string>` For example, `trapsink 10.94.174.190 public`.
6. Start the SNMP services (`service snmpd restart`).

Installing SNMP Tools (Windows Server 2012 Or Later)

By default, in Windows Server 2012 or later, the SNMP configuration options are disabled. You must install SNMP tools to view the **Security** and **Traps** tabs in the **SNMP Service Properties** window.

1. Open **Server Manager**.
2. Click **Manage** → **Add roles and features**.
   The **Add Roles and Features Wizard** is displayed.
3. Click **Next** until you navigate to **Server Selection**.
4. Under **Server Pool**, select the local server as the destination server and click **Next**.
5. In **Features**, select **Remote Server Administrator Tools** → **Feature Administration Tools** → **SNMP Tools** and click **Next**.
6. Click **Install**.
7. In a command prompt, type `services.msc` and press <Enter> to open the **Services** window.
8. Right-click **SNMP Service** and click **Restart**.
9. Close the **Services** window.
10. Open the **Services** window again, right-click **SNMP Service** and click **Properties**.
11. Ensure that the **Security** and **Traps** tab are displayed in the **SNMP Service Properties** window.

Enabling Network Discovery (Windows Server 2008 Only)

On all managed nodes running Windows Server 2008, enable network discovery to allow the nodes to be discovered by the management server.

1. Click **Start** → **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change advanced sharing settings**.
2. Choose the drop-down arrow for the applicable network profile (**Home or Work**, or **Public**).
3. Under **Network discovery**, select **Turn on network discovery**.
4. Click **Save changes**.

Setting Up SupportAssist

To set up SupportAssist in your environment:

NOTE: For information on the prerequisites and minimum requirements for installing and using SupportAssist, see the *Dell SupportAssist Version 1.3 For Dell OpenManage Essentials User's Guide* at **dell.com/ServiceabilityTools**.

1. Ensure that SupportAssist version 1.3 is installed on the management server running OpenManage Essentials version 1.3.
2. Confirm if the registration of the SupportAssist application is successful. If the registration is successful:
   - The primary contact receives the SupportAssist registration confirmation email.
   - The **Help** → **About** window in SupportAssist displays a **Client ID** value.

   If the registration fails, a message is displayed in the **First-Time Setup** window. Registration failure occurs if the SupportAssist application has problems communicating with the SupportAssist server hosted by Dell. To resolve the communication problems, see Ensuring Successful Communication Between The SupportAssist Application And The SupportAssist Server.

3. Perform the connectivity test to verify if the SupportAssist application is able to communicate successfully with the SupportAssist server hosted by Dell. See Testing SupportAssist Connectivity.
4. Verify the installation of the collection tools. See Verifying The Installation Of The Collection Tools.
5. Configure the Administrator credentials of each supported device type in your environment in SupportAssist. See Configuring The Default Device Type Credentials.
6. If the devices in your environment are covered under the Dell ProSupport Plus service contract, configure SupportAssist to collect the system logs periodically. See Configuring Periodic Collection Of System Logs.
7. For monitoring Dell Force10 switch/router only — If you had discovered and inventoried Force10 switch/router in OpenManage Essentials version 1.2, and then upgraded to OpenManage Essentials version 1.3, you must rediscover the Force10 switch/router in OpenManage Essentials. For information on discovering devices in OpenManage Essentials, see the *Dell OpenManage Essentials Version 1.3 User's Guide* at **dell.com/OpenManageManuals**.
8. Verify if the SupportAssist application is able to generate the system log collection and upload it to Dell successfully. See Verifying the System Log Collection Or Upload Configuration.
9. If you want to automatically download and install the latest SupportAssist and collection tool updates when they are available, enable auto update. See Enabling Auto Update.

   NOTE: In SupportAssist version 1.1.1, the PowerEdge VRTX device is displayed as an iDRAC7 device. After upgrading SupportAssist from version 1.1.1 to 1.3, the PowerEdge VRTX device continues to display as an iDRAC7 device. To ensure that the PowerEdge VRTX device is displayed as expected after the upgrade, in OpenManage Essentials, remove the PowerEdge VRTX device and discover it again.

Ensuring Successful Communication Between The SupportAssist Application And The SupportAssist Server

To ensure that the SupportAssist application is able to successfully communicate with the SupportAssist server:

- The management server on which the SupportAssist application is installed must be able to connect to the following destinations:
  - **https://api.dell.com/support/case/v2/WebCase** — end point for the SupportAssist server. On the management server, verify if you can access the following location using the web browser: **https://api.dell.com/support/case/v2/WebCase?wsdl**.
  - **https://ddldropbox.us.dell.com/upload.ashx/** — the file upload server where the diagnostic test results are uploaded. Verify if the server certificate on **ddldropbox.us.dell.com** is valid. See Verifying The Server Certificate.
  - **https://ftp.dell.com/** — for getting SupportAssist update information. On the management server, verify if you can access the following location using the web browser: **https://ftp.dell.com/**.
- Verify if port 443 is open on the management server for **ddldropbox.us.dell.com** and **ftp.dell.com**. You can use a telnet client to test the connection. For example, you can use the following command: `o ddldropbox.us.dell.com 443`.
- Verify if the network settings on the management server are correct.
- If the management server on which SupportAssist is installed connects to the Internet through a proxy server, configure the proxy settings in SupportAssist. To configure the proxy settings, click **Settings** → **Proxy Settings** and provide the proxy details.

  NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

If the communication problem persists, contact the network administrator for further assistance.

Verifying The Server Certificate

To verify the server certificate on **ddldropbox.us.dell.com** using Internet Explorer:

1. Open **https://ddldropbox.us.dell.com** .
   A **404 — File or directory not found** error may be displayed.
2. On the address bar, click the **Security Report** icon , and then click **View Certificates**.
   The **Certificate** is displayed.
3. In the **General** tab, verify if the certificate displays a valid date.
4. Click the **Certification Path** tab, and verify if the **GTE CyberTrust Global Root** certificate is listed.

Testing SupportAssist Connectivity

The connectivity test enables you to test communication between the SupportAssist application and the SupportAssist server hosted by Dell.

To test the connectivity:

NOTE: The **Connectivity Test** link is enabled only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

1. In SupportAssist, move the mouse pointer over the **<user name>** link that is displayed beside the **Help** link, and then click **Connectivity Test**.
2. In the **Connectivity Test** page, click **Send**.
   The SupportAssist server receives the connectivity test, and sends a sample email with connectivity status to the primary and secondary (optional) contact. If the connectivity status email is not received, see the troubleshooting instructions in Connectivity Test Failure.

Verifying The Installation Of The Collection Tools

SupportAssist uses the following collection tools to generate the system log collection from supported devices in the environment:

- Dell System E-Support Tool (DSET)
- Dell Lasso

The collection tools are automatically downloaded and installed in the background after the installation of SupportAssist. To successfully generate the system log collection, the collection tools must be of a version that is compatible with SupportAssist.

To verify if a compatible version of the collection tool is installed:

1. Navigate to the **Control Panel**.
2. Click **Programs** → **Programs and Features**.
   The **Uninstall or change a program** window is displayed.
3. In the list of installed applications, verify if the compatible version of DSET and Lasso are installed.

   NOTE: For information on the version of DSET and Lasso that is compatible with SupportAssist, see the *Dell SupportAssist For Dell OpenManage Essentials Support Matrix* or the *Dell SupportAssist For Dell OpenManage Essentials Release Notes* at **dell.com/ServiceabilityTools**.

If the collection tools are not installed, click the **Update Available** link displayed in the SupportAssist header. The collection tools will be downloaded and installed in the background.

NOTE: The **Update Available** link is displayed only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

Configuring The Default Device Type Credentials

SupportAssist runs the appropriate collection tools and gathers the system log collection when a hardware issue is detected in your environment. To run the collection tools on the supported devices, you must configure SupportAssist with the Administrator credentials for each managed device type.

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

NOTE: Whenever the Administrator credentials of supported devices are changed, you must ensure that the **Default Device Type Credentials** are also updated in SupportAssist. Alternately, you can create a service account that never expires, and provide the service account credentials in SupportAssist.

For example, if the managed PowerEdge servers are part of a domain, you can create a service account on the domain controller, and add the service account to the Local Administrators group of the managed server. Then provide the service account credentials in the **Default Device Type Credentials** page in SupportAssist. For more information, see the *Managing Device Credentials in SupportAssist Using Service Account* technical white paper at **dell.com/SupportAssistGroup**.

1. Click the **Settings** tab.
2. Under **Edit Device Type Credentials**, select the **Device Type** and **Credential Type**.
3. Type the Administrator credentials [**Username**, **Password**, **Enable Password** (for Ethernet switches only), and **Community String** (for Dell EqualLogic storage arrays and EqualLogic FluidFS NAS appliances only)] of the selected **Device Type** and **Credential Type** in the corresponding fields.

   NOTE: Windows user names must be of the form [Domain\Username]. You can also use a period [.] to indicate the local domain. This rule does not apply to Linux or ESX/ESXi credentials.

   NOTE: For EqualLogic FluidFS NAS appliances, you must provide the EqualLogic SAN credentials.

   NOTE: For Force10 and PowerConnect Ethernet switches the domain name need not be specified.

   Examples of Windows user names: `.\Administrator; MyDomain\MyUsername`.

   Example of Linux or ESX/ESXi user name: `Username`.
4. Repeat step 2 and step 3 until you have configured the **Default Device Type Credentials** for each managed device type.
5. Click **Save Changes**.

   NOTE: If the credentials for a device differs from the **Default Device Type Credentials** you provided, you can edit the credentials for that particular device. To edit the credentials for a device, select the device in the **Devices** tab, click **Edit Device Credentials**, and provide the details.
6. Verify if SupportAssist is able to generate the system log collection and upload it to Dell for each **Device Type** and **Credential Type** you have configured. See Verifying The System Log Collection Or Upload Configuration.

Configuring Periodic Collection Of System Logs

To receive the full benefits of the support, reporting, and maintenance offering of your ProSupport Plus service contract, you must configure SupportAssist to collect the system logs at periodic intervals for each supported device type.

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

1. Click the **Settings** tab.
2. Click **Preferences**.
   The **Email Settings**, **Support Collection**, and **Maintenance Mode** page is displayed.
3. Under **Support Collection**, ensure that **Enable scheduling** is selected.
4. Click **System Logs**.
   The **System Logs** page is displayed.
5. Under **Edit Device Credentials**, select the **Device Type** and **Credential Type**.
6. Verify or provide the credentials (**Username**, **Password**, **Confirm Password**, and **Community String**) for the selected credential type. For more information, see Configuring The Default Device Type Credentials.
7. Under **System Log Collection Schedule**, set the **Frequency**, and select the appropriate fields in **Specify day and time**.

   NOTE: For recommendations on setting the frequency of periodic collection, see Network Bandwidth Consumption And Recommendations For Scheduling Periodic Collection.
8. Repeat step 5 to step 7 until you have scheduled the collection of system logs for all supported device types in your environment.
9. Click **Save Changes**.

Network Bandwidth Consumption And Recommendations For Scheduling Periodic Collection

NOTE: In an environment that consists of less than 300 devices, the network bandwidth consumed for uploading the system log collection is about 4 MB/second.

The following table provides information about network bandwidth consumption and recommendations for scheduling periodic collections in an environment that consists of 75 percent servers and 25 percent switch and storage devices. The recommendations also assume compliance with the hardware, software, and networking requirements for SupportAssist.

Total number of devices	Network bandwidth consumed for uploading the collection (GB/month)	Time taken for generating the collection (hours)	Recommendations for scheduling periodic collection
Less than 300	16	20	Weekly (overnight)
300 or more	7.2 to 47	22.5	For EqualLogic and Force10 devices — Weekly (overnight) For Dell PowerEdge and Dell PowerConnect devices — Monthly (at different times during

Total number of devices	Network bandwidth consumed for uploading the collection (GB/month)	Time taken for generating the collection (hours)	Recommendations for scheduling periodic collection
			the week for each device type)

Verifying The System Log Collection Or Upload Configuration

To verify that SupportAssist is correctly configured to generate the system logs and upload it to Dell:

1. Click the **Devices** tab.
   The **Device Inventory** page is displayed.
2. Select a device in the **Device Inventory**.

   NOTE: The **Send System Logs** link is enabled only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

   The **Send System Logs** link is enabled.
3. Click **Send System Logs**.
   The status of the system log collection is displayed in the **Collection Status** column.
4. To add other devices to the system log collection queue, select each device in the **Device Inventory**, and then click **Send System Logs**.

When SupportAssist is able to successfully generate the system log collection and upload it to Dell, the **Collection Status** column displays **Collection Uploaded**. For information on troubleshooting problems with the generation and upload of the system log collection, see Collection Failure and Collection Upload Failure.

Enabling Auto Update

To enable auto update:

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

1. Click the **Settings** tab.
   The **System Logs** page is displayed.
2. Click **Preferences**.
   The **Auto Update**, **Email Settings**, **Support Collection**, and **Maintenance Mode** page is displayed.
3. Under **Auto Update**, select **Enable auto update**.
4. Click **Save Changes**.

Troubleshooting

This section provides information required to troubleshoot the following:

- Registration Failure
- Collection Failure
- Collection Upload Failure
- Connectivity Test Failure

Registration Failure

After the installation of SupportAssist application on the management server, the SupportAssist application registers with the SupportAssist server hosted by Dell. If the registration is successful:

- A registration confirmation email is sent to your primary contact.
- The **Help** → **About** window in SupportAssist displays a **Client ID** value.

If the registration fails, a message is displayed in the **First-Time Setup** window. Registration failure occurs if the SupportAssist application has problems communicating with the SupportAssist server hosted by Dell. To resolve the communication problems, see Ensuring Successful Communication Between The SupportAssist Application And The SupportAssist Server.

Collection Failure

If you receive a SupportAssist email notification indicating a collection issue with a specific device and the **Collection Status** of the device displays **Failed to Run**:

1. Verify if the device is connected to the network.
2. Verify the credentials you have provided for the device. You must provide the Administrator credentials in the **Settings** → **System Logs** page. For more information, see Configuring The Default Device Type Credentials. If you want to edit the credentials for a particular device, select the device in the **Devices** tab, click **Edit Device Credentials**, and provide the details.
3. Verify if the DNS is configured with the host name of the device. If you do not have a DNS server in your environment, on the management server, update the hosts file located at **C:\Windows \System32\drivers\etc** with the IP address and the corresponding host name.

Collection Upload Failure

If you receive a SupportAssist email notification indicating an issue uploading the collection for a specific device and the **Collections Status** of the device displays **Collection Failed to Upload**:

1. Verify if the management server on which SupportAssist is installed is able to connect to the Internet.
2. If management server on which SupportAssist is installed connects to the Internet through a proxy server, ensure that you configure the proxy settings in SupportAssist. To configure the proxy settings, click **Settings** → **Proxy Settings** and provide the proxy details.
3. Perform the connectivity test and ensure that the test is successful. See Testing SupportAssist Connectivity.
4. Verify if the SupportAssist application is able to successfully communicate with the SupportAssist server. See Ensuring Successful Communication Between The SupportAssist Application And The SupportAssist Server.

After resolving the issue, manually upload a new collection for the device to Dell. To manually upload the collection, see Sending The System Logs Manually.

Sending The System Logs Manually

To send the system logs manually:

NOTE: The **Send System Logs** option is enabled only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

1. Click the **Devices** tab.
   The **Device Inventory** is displayed.
2. Select the device in the **Device Inventory** table.
   The **Send System Logs** link is enabled.
3. Click **Send System Logs**.
   The **Collection Status** column in the **Device Inventory** displays the status of the collection and upload of the system logs.

Connectivity Test Failure

The connectivity test may fail due to:

- Proxy settings — If your network requires passing the web browser traffic through a proxy server, ensure that the proxy is enabled and configured in SupportAssist.
- SSL connection failure — If the proxy settings are configured properly, but the connectivity test fails, there may be a SSL connection failure.

If there is a SSL connection failure, you must install the required root certificates. To identify and resolve SSL connection failure, see Identifying SSL Connection Failure and Installing Root Certificates.

Identifying SSL Connection Failure

SSL connection failure may occur if the system does not have the required certificate installed from the issuing root certificate authority, GTE CyberTrust Global Root. All Dell certificates are issued from this certificate authority.

To verify if the certificate is installed in Internet Explorer:

1. Click **Tools → Internet Options**.
   The **Internet Options** dialog box is displayed.
2. Click the **Content** tab, and then click **Certificates**.
   The **Certificates** dialog box is displayed.
3. Click the **Trusted Root Certification Authorities** tab.
4. Scroll to verify if **GTE CyberTrust Global Root** is listed in the **Issued To** and **Issued By** columns.

If **GTE CyberTrust Global Root** is not listed, you must install the required certificates. See Exporting The Root Certificate and Installing The Root Certificate.

Exporting The Root Certificate

To export the root certificate:

1. In Internet Explorer, go to **https://dell.com**.
2. If the **Certificate Error: Navigation Blocked** page is displayed, click **Continue to this website (not recommended)**.
3. At the **Do you want to view only the webpage content that was delivered securely?** prompt, click **Yes**.
4. On the address bar, click the **Security Report** icon .

5. Click **View certificates**.
   The **Certificate** window is displayed.
6. Click **Details**.
7. Click **Copy to File**.
   The **Certificate Export Wizard** is displayed.
8. Click **Next**.
9. In the **Export File Format** page, click **Next**.
10. In the **File to Export** page, click **Browse**.
    The **Save As** window is displayed.
11. Navigate to the location you want to save the certificate file.
12. Type a file name and click **Save**.
13. In the **Export File Format** page, click **Next**.
14. Click **Finish**.
    The status of the export is displayed.
15. Click **OK**.

Installing The Root Certificate

Before you begin, ensure that:

- You are logged in using the user account with which SupportAssist was installed.
- You have administrator privileges.
- The SupportAssist service is running.
- You have exported the certificate file. See Exporting The Root Certificate.

To install the root certificate:

1. Click **Start** → **Run**.
   The **Run** dialog box is displayed.
2. In the **Open** box, type `mmc` and click **OK**.
   The **Console1 – [Console Root]** window is displayed.
3. Click **File** → **Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box is displayed.
4. Under **Available snap-ins**, select **Certificates**, and click **Add >**.
   The **Certificates snap-in** dialog box is displayed.
5. Ensure that **My user account** is selected, and then click **Finish**.
6. In the **Add or Remove snap-ins** dialog box, click **Add >**.
   The **Certificates snap-in** dialog box is displayed.
7. Select **Computer account** and click **Next**.
   The **Select Computer** dialog box is displayed.
8. Ensure that **Local computer: (the computer this console is running on)** is selected and click **Finish**.
9. In the **Add or Remove snap-ins** dialog box, click **OK**.
10. Under the **Console Root**, click **Certificates – Current User**.
11. Right-click **Trusted Root Certification Authorities** → **All Tasks** → **Import**.
    The **Certificate Import Wizard** is displayed.
12. Click **Next**.
    The **File to Import** dialog box is displayed.

13. Browse to select the exported certificate file and click **Next**.
    The **Certificate Store** information is displayed.
14. Click **Next**.
15. Click **Finish**.
16. Right-click **Intermediate Certification Authorities → All Tasks → Import**.
    The **Certificate Import Wizard** is displayed.
17. Browse to select the exported certificate file and click **Next**.
    The **Certificate Store** information is displayed.
18. Click **Next**.
19. Click **Finish**.
20. Under the **Console Root**, click **Certificates (Local Computer)**.
21. Perform step 11 to step 19 to install the root certificate.